AO 106 (Rev. 01/09) Application for a Search Warrant

United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Email Account: Imanager@consultant.com

Case No. 17-MJ-1161

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Email account: Imanager@consultant.com, stored at premises owned, maintained, controlled, or operated by 1&1 Mail & Media, Inc., a company located at 701 Lee Road, Suite 300, Chesterbrook, PA 19087

which is more fully described in Attachment A, which is attached hereto and incorporated herein by reference, there is now concealed *(identify the person or describe the property to be seized)*:

The items set forth on the attached Items to be Seized, more fully described in Attachment B, which is attached hereto and incorporated herein by reference;

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of 18 U.S.C. Section 1343.
The application is based on these facts:

- ☒ continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Joseph Crean, Task Force Agent
Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.
Date: November 28, 2017

Judge's signature

City and state: Buffalo, New York

JEREMIAH J. McCARTHY
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Joseph Crean, being first duly sworn, hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Police Officer with the Cheektowaga Police Department since August 30, 1990. I am currently assigned to the Federal Bureau of Investigation (F.B.I.) Cyber Squad, Buffalo Division, New York. I have been assigned to the F.B.I. Cyber Squad Buffalo Division since October 2016. As part of the Cyber Squad, I work on investigations relating to criminal cyber intrusions and cyber fraud. I have gained experience through training and everyday work related to these types of investigations. During my tenure with the F.B.I. Task Force, I have also worked on other investigations to include wire fraud investigations. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with F.B.I. Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with various criminal investigations.

2. I make this affidavit in support of an application for a search warrant authorizing the search of an email account, IMANAGER@CONSULTANT.COM, controlled by the service provider known as: 1&1 Mail & Media, Inc., headquartered at 701 Lee Road, Suite 300 Chesterbrook, PA 19087.

3. The email account and the information to be searched are described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Service Provider to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including contents of communications.

4. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1343 [Wire Fraud] will be found in the account: IMANAGER@CONSULTANT.COM.

5. In my training and experience, I have learned that 1&1 Mail & Media, Inc. is a company that provides Internet electronic mail (email) access to the public, and that stored electronic communications, including opened and unopened email for subscribers, may be located on the computers owned or leased by these companies. Further, I am aware that computers located at 1&1 Mail & Media. Inc. contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein.

6. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, and information provided by other private companies. Because this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facility.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. On or about February 23, 2017, the FBI received a complaint from Eastman Machine Company, located at 77 Washington Street, Buffalo, New York, regarding fraud.

9. On Tuesday, February 21, 2017, the IT Manager for Eastman Machine Company received a quote from Dell for purchasing computers. The quote was for eight computers at a total cost of $12,336.40. Eastman Machine Company did not attempt to purchase computers from Dell.

10. On Wednesday, February 22, 2017, the IT Manager contacted Dell and learned someone tried to purchase computers using Eastman Machine Company's line of credit by impersonating him.

11. On Wednesday February 23, 2017, the IT Manager became aware of a second attempt to purchase computers from Southern Computer Warehouse, Marietta, Georgia. During that attempt, the suspect tried to open a line of credit in the name of Eastman Machine Company, again impersonating the IT Manager. As part of the scheme, the suspect used the address of Greater Buffalo Savings Bank, a bank with which Eastman Machine Company

held an account in the past. The suspect tried to order 5 computers at a cost of $9,631.99. The intended recipient was Cecilia Wu, with a known address in Brooklyn, NY.[1]

12. Furthermore, Eastman Machine Company reported that three domains were created without knowledge or consent from the company. A domain is the address of a web site, such as *Eastmancuts.com*, which belongs to Eastman Machine Company. The person who set up the fraudulent domains set them up in a way to closely resemble the true company domain of *Eastmancuts.com*. More specifically, the fraudulent domains included Eastmancuts.net, Eastmancut.com, and Eastmanscut.com, which are hosted by 1and1.com. When accessed, the fraudulent domains would direct a browser to a different website where customer information was obtained and later used for fraudulent purchases on other web sites. For example, on March 8, 2017, the Eastman Machine Company IT Manager became aware that the fraudulent domain Eastmancut.com did attempt to obtain a line of credit from Vology.com. On March 10, 2017, Eastman Machine Company IT Manager became aware that the suspect attempted to use the fraudulent domain Eastmancut.com to order merchandise from Fireflyadvantage.com and MNJ Technologies.

13. On March 16, 2017, the Eastman Machine Company IT Manager received a quote from American II Electronics with the aforementioned shipping address associated with Cecilia Wu, and a contact of IMANAGER@CONSULTANT.COM. The IT Manager confirmed that Eastman Machine Company did not attempt to make a purchase from American II Electronics.

[1] The address can be disclosed to the Court should the Court require.

14. On August 14, 2017, New York City based Task Force Officer Michael Eddi interviewed Cecilia Wu. Wu provided that her previous boyfriend introduced her to her new boss, Jeremy Cheng, who uses email address IMANAGER@CONSULTANT.COM. Cecilia Wu stated that Jeremy Cheng emails her using IMANAGER@CONSULTANT.COM, and directs Wu on what to do with deliveries. Cheng also wires money to her bank account. Wu stated that Cheng works in Sweden, and directs Wu to reship packages for him, mostly overseas, to Georgia, to Texas, and to South Africa. Cheng wires money into Wu's account (Webster Bank, based in Younkers, NY), which she then wires via MoneyGram to additional mules who also receive packages and money wires on Cheng's behalf. Recently, Wu has been reshipping packages approximately 2-3 times a month to 2-3 times a week, mostly Dell computers. Wu further provided printouts of emails and invoices/shipping labels sent to her by Cheng. Wu advised Task Force Officer Eddi that she knew that the activity that she was involved in was wrong but Wu stated that she needed the money. Wu provided 12 emails associated with the fraudulent activity from IMANAGER@CONSULTANT.COM dated from June 1, 2015, until March 20, 2017, all of which she indicated were associated with fraudulent transactions.

15. A subpoena return for the email account IMANAGER@CONSULTANT.COM from 1&1 Mail & Media Inc. did not identify Jeremy Cheng as the subscriber. Rather, the return identified an individual with initials MG.

16. Based on the Affiant's training and expertise combined with research associated with this investigation, your Affiant believes that the suspect used email address IMANAGER@CONSULTANT.COM in furtherance of this scheme to defraud. Based on the facts previously stated, there is probable cause to believe that the 1&1 Mail & Media, Inc.

account IMANAGER@CONSULTANT.COM was used in the furtherance of the above outlined scheme to defraud.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFADIVAT

17. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

18. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is

attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

19. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

20. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format."

BACKGROUND REGARDING 1&1 Mail & Media, Inc.

21. Based on my training and experience, I have learned the following about 1&1 Mail & Media, Inc.:

d. 1&1 Mail & Media, Inc. is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18,United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by

registering on the Internet with 1&1 Mail & Media, Inc. 1&1 Mail & Media, Inc. requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, 1&1 Mail & Media, Inc. does not verify the information provided. As part of its services, 1&1 Mail & Media, Inc. also provides its subscribers with the ability to set up email accounts;

e. 1&1 Mail & Media, Inc. maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information;

f. Subscribers to 1&1 Mail & Media, Inc. may access their accounts on servers maintained or owned by 1&1 Mail & Media, Inc. from any computer connected to the Internet located anywhere in the world;

g. Any email that is sent to a 1&1 Mail & Media, Inc. subscriber is stored in the subscriber's "mail box" on 1&1 Mail & Media, Inc. servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on 1&1 Mail & Media, Inc. servers indefinitely;

h. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to 1&1 Mail & Media, Inc. servers, and then transmitted to its end destination. 1&1 Mail & Media, Inc. users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email

from the 1&1 Mail & Media, Inc. server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at 1&1 Mail & Media, Inc., but that message will remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;

i. A 1&1 Mail & Media, Inc. subscriber can store files, including emails and image files, on servers maintained and/or owned by 1&1 Mail & Media, Inc.; and

j. Emails and image files stored on a 1&1 Mail & Media, Inc. server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the 1&1 Mail & Media, Inc. server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the 1&1 Mail & Media, Inc. servers.

22. An 1&1 Mail & Media, Inc. subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by 1&1 Mail & Media, Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

23. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

24. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and

timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Service Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I in Attachment B annexed hereto. Because the Service Providers are not aware of the facts of this investigation, their employees are not in a position to search for relevant evidence. In addition, requiring the Service Providers to perform the search would be a burden upon the companies. If all the Service Providers were asked to do was produce all the files associated with the account, an employee can do that easily. Requiring the Service Providers to search the materials to determine what content is relevant would add to their burden. Upon receipt of the information described in Section I in Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

28. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the email accounts located on computer systems owned, maintained, and/or operated by1&1 Mail & Media, Inc. there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 [Wire Fraud]. I therefore respectfully request that the Court issue a search warrant directed to the Service Provider for the email account identified in Attachment A for information described in Attachment B. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

29. Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal for 60 days, without prejudice to the Government's right to seek a further extension.

REQUEST FOR ORDER COMMANDING PROVIDERS NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF THE WARRANT

30. The United States requests that the Court order the Provider not to notify any person, including the subscribers and customers of the accounts listed in the warrant, of the existence of the attached warrant until 30 days after the date of execution.

31. 1&1 Mail & Media, Inc. is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15). Pursuant to 18 U.S.C. § 2703, the United States is seeking the attached warrant requiring the Provider to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.*

32. In this case, such an order would be appropriate because the attached warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, or endanger the life or physical safety of an individual. *See* 18 U.S.C. § 2705(b). Some of the evidence in this investigation is stored electronically. If alerted to the existence of the warrant, the subjects under investigation could destroy that evidence, including information saved to their personal

computers. Wherefore, the United States respectfully requests that the Court grant the attached Order directing the Providers not to disclose the existence or content of the attached warrant until 30 days after the date of execution, except that the Providers may disclose the attached warrant to an attorney for the Providers for the purpose of receiving legal advice.

JOSEPH CREAN
Task Force Officer
Federal Bureau of Investigation

Sworn to before me this 28TH
day of November, 2017.

JEREMIAH J. McCARTHY
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with email account IMANAGER@CONSULTANT.COM, stored at premises owned, maintained, controlled, or operated by 1&1 Mail & Media Inc., a company located at 701 Lee Rd., Suite 300 Chesterbrook, PA 19087.

ATTACHMENT B

I. Information to be disclosed by 1&1 Mail & Media Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of 1&1 Mail & Media Inc., 1&1 Mail & Media Inc., is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. For the time period of May 1, 2015, to the present, the contents of all emails stored in the account, including copies of emails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any creditor bank account number);

c. For the time period of May 1, 2015, to the present, all records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All content in the Docs, Calendar, Friend Contacts and Photos areas;

e. For the time period of May 1, 2015, to the present, any and all files linked to email accounts of the user; and

h. For the time period of May 1, 2015, to the present, all records pertaining to communications between 1&1 Mail & Media and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 [Wire Fraud], for each account or identifier listed on Attachment A.